

# Larkのデータセキュリティへの取り組み

IT管理者のためのユーザー保護ガイド



# 目次

はじめに .....	1
1. セキュリティチームとその機能 .....	1
2. コンプライアンスとプライバシー保護 .....	1
3. 従業員のセキュリティ .....	2
4. アプリのセキュリティ .....	3
4.1 運用環境のセキュリティ .....	3
4.2 データセキュリティ .....	3
4.3 セキュリティの脆弱性保護 .....	3
4.4 クライアントのセキュリティ戦略 .....	3
5. ネットワークのセキュリティ .....	3
5.1 ネットワークのアクセス管理 .....	3
5.2 DDoS攻撃とサイバー攻撃からの防御 .....	4
5.3 ネットワーク通信の暗号化 .....	4
6. サーバーセキュリティ .....	4
7. アプリケーションのセキュリティ .....	4
7.1 セキュリティ開発のプロセス .....	4
7.2 ユーザーアカウントのセキュリティ .....	5
7.3 脆弱性と緊急対応 .....	5
8. データセキュリティ .....	5
8.1 データ通信 .....	5
8.1 データストレージ .....	5
8.1 データアクセス .....	6
8.4 データの削除 .....	6
8.5 データへの不正侵入検知 .....	7
9. 物理インフラストラクチャーのセキュリティ .....	7
9.1 アマゾン ウェブ サービス (AWS) インフラストラクチャーのセキュリティ .....	7
9.2 アカマイ インフラストラクチャーのセキュリティ .....	7
10. 障害回復とサービス継続性 .....	8
10.1 バックアップと障害回復 .....	8
10.2 サービス継続性の保証 .....	8

10.3 緊急訓練 .....	8
11. 変更管理 .....	8
11.1 プログラムの変更 .....	8
11.2 ソースコードの管理 .....	9
11.3 ITインフラストラクチャーの変更 .....	9
11.4 モニタリングの変更 .....	9

# はじめに

Larkの新世代オフィススイートSaaS「Larkスイート」は、さまざまな便利な機能を集約し、あらゆるデバイスに柔軟に対応して、リアルタイムのコラボレーションを可能にします。ユーザーの作業効率を高め、生産や管理に必要なコストを削減し、より安全でスマートなビジネス環境を実現します。

さらにLarkは、情報技術とアプリケーションシステムをLarkスイートの開発と運用に活用しています。

「Larkスイート」は、Lark Technologies Pte. Ltd.（以下「当社」）によって開発されたSaaSサービスの企業向けオフィススイートで、インスタントメッセージ、クラウドドキュメント、スマートカレンダー、ビデオ会議、オープンプラットフォームなどの豊富な機能を搭載しています。Larkスイートは業界をリードするテクノロジーのセーフガードを利用し、データライフサイクル全体を通じて製品とユーザーデータの保護を保証するためのセキュリティ対策を行っています。Larkスイートの設計、開発、運用は、コンプライアンスやセキュリティに関する基準を満たして実施されています。

## 1. セキュリティチームとその機能

SaaSサービスプロバイダーとして、Larkはユーザーサービスとデータのセキュリティを最優先事項としています。当社は、完全なセキュリティインフラストラクチャーと、ユーザーサービス、データセキュリティ保護システムを有しています。Larkのセキュリティチームは、セキュリティ管理とコンプライアンス、ビジネスセキュリティ、データセキュリティ、緊急対応、セキュリティツール開発といった分野を担当するチームで構成されています。各チームは製品設計のセキュリティ評価、コードセキュリティレビュー、脆弱性スキャン、侵入テスト、脅威インテリジェンス、侵入検知、緊急対応、データセキュリティ、セキュリティコンプライアンスなどに取り組んでいます。

## 2. コンプライアンスとプライバシー保護

Larkは製品コンプライアンスを重視しており、当社のセキュリティおよびコンプライアンス部門は、国内外の最高基準のコンプライアンスを実施する責任を負っています。Larkにはプライバシーの保護に専門的に取り組むチームがあり、ユーザープライバシープロトコル、製品プライバシー保護の設計、ユーザーデータの収集と使用を管理し、ユーザーデータが正しく使用・処理されているか、また、それに合理性や透明性があるかを確認します。

当社は、製品コンプライアンスに関する国際的な要件を遵守しており、さまざまな規制機関と協力して製品およびサービスが要件を満たしていることを確認しています。

Larkは、情報セキュリティ管理に関する国際規格の1つである「ISO27001認証」を取得しています。これは、世界で最も権威があり、また、最も厳しい情報セキュリティシステム認証基準の1つです。Larkのデータセンター、管理システム、R&D、および機能部門はこの認証をクリアしています。これは、当社は情報セキュリティ管理の国際基準を満たし、世界中で安全で信頼できる顧客サービスを提供するのに十分な情報セキュリティリスクの識別および制御機能を備えていることを意味します。

また、Larkはパブリッククラウド上の個人情報保護に関する国際規格「ISO27018認証」を取得しました。この規格は、パブリッククラウドにおける個人識別情報（PII）の

セキュリティ保護策の実施規範について定めたガイドラインです。このISO27018認証を取得していることで、Larkが企業データの保護、ユーザーの個人情報の保護、および情報漏えいの防止において高い基準を達成したことを証明しています。

Larkは、PDCAの完全なクローズドループを備えたプライベートな情報の管理のためのシステムに関する基準である「ISO27701認証」を取得しています。これは27001および27002を拡張する基準で、プライバシー情報管理システムを確立、導入、維持し、継続的に改善するための要件を定めています。個人識別情報（PII）の処理に必要なプライバシー保護は、情報セキュリティ保護に基づいて実施されます。Larkは、世界クラスのプライバシーコンプライアンスシステムを構築するための長期的な取り組みに対するコミットメントとして、この認定を取得しました。

Larkは、「SOC 2 Type I」、「SOC 2 Type II」、およびSOC 3のサービス監査報告書を取得しています。「SOC (System and Organization Controls) 報告書」は、米国公認会計士協会（AICPA）の関連ガイドラインに基づいた、専門の第三者会計事務所により発行された、組織の内部統制に関する独立試験報告書です。その中の1つである「SOC2」は、国際的なトラストサービスの原則と基準（セキュリティ、可用性、処理の整合性、機密性、プライバシー）に基づいて顧客データを管理するための基準を定義しています。Larkのサービスや製品は、この基準を満たしていることを確認するために第三者によって定期的に監査されており、これは当社が常に信頼性と安全性を確保したサービスを提供していることを示しています。顧客データを安全に管理し、組織の利益と顧客のプライバシーを保護できます。

この認定は、Larkが情報セキュリティやサービスの品質、ITサービス管理などにおいて一定の基準を満たした管理を実施していることを示し、当社の品質システムの改善と完成のための強固な基盤を築きます。

### 3. 従業員のセキュリティ

Larkは、安全に人材管理を行うプロセスを確立しています。

- ・新入社員の採用は、人事（HR）スペシャリストや、リソースを必要とする部門のリーダーによる承認が必要です。そして、その採用プロセスと結果は、人事管理システムに記録されます。
- ・新入社員を雇用する前に、人事部は従業員の役職に応じて居住国の法律および規制に従って身元調査を行い、その採用が当社の規則および規制を十分に満たしているかを確認する必要があります。
- ・新規に雇用された従業員は、情報のセキュリティに関する義務と責任について示した雇用契約と機密保持契約に署名する必要があります。
- ・法務部は、従業員および第三者との間で結ぶ機密保持契約に含まれる法的条件を年に最低1回レビューし、必要に応じて更新を行い、社内の知識プラットフォームを通じて更新された契約を公開します。これにより、すべての従業員と関係者が最新の機密保持契約にアクセスできるようにします。
- ・従業員の辞任は、従業員自身または人事管理システムの部門リーダーが当事者の意思を表明し、人事部、IT部門などから承認を得た後に正式に辞任が成立します。

Larkはさまざまなスキルの包括的なトレーニングおよび学習システムを確立しています。新規雇用の従業員は、企業文化、規則と規制、情報セキュリティ、および報酬と処罰の仕組みに関するトレーニングへの参加が課されます。その一方で、Larkは従業員の専門知識とスキル、および情報セキュリティに対する知識や認識を強化するために以下を実施しています。

- ・従業員の情報セキュリティスキルを強化するための情報セキュリティ関連のトレーニング
- ・情報セキュリティの意識向上を促進するための情報セキュリティ活動
- ・セキュリティ意識に関連する資料を準備し、メールや社内の掲示などを介して従業員に配信

## 4. アプリのセキュリティ

### 1. 運用環境のセキュリティ

Larkアプリケーションは、ルート検出、ジェイルブレイクの検出、バグ・欠陥の検出、インジェクションの検出などを含む稼働環境の厳密なスクリーニングテストを行います。テストの目的は、アプリがハッキングされたりマルウェアに感染した場合にも、ユーザーが安全で信頼できる環境でサービスを利用できるようにすることです。

### 2. データセキュリティ

Larkアプリケーションは、オペレーティングシステムのセキュリティメカニズムを利用して、アプリ間で権限を分けます。クライアント情報は暗号化され、保管されます。クライアントとサーバー間で行われるすべての通信は、HTTPSまたはWSSで暗号化されます。

### 3. セキュリティの脆弱性保護

Larkにはモバイルセキュリティ脆弱性のマイニングチームがあり、Android、iOS、Windows、macOSクライアントのセキュリティ評価と脆弱性マイニングを行っています。クライアントのサードパーティコンポーネント（ライブラリまたはSDK）の脆弱性の検出と、既存のアプリケーションの脆弱性を可能な限り排除し、クライアントのセキュリティを確保します。

### 4. クライアントのセキュリティ戦略

顧客の管理担当者は、管理コンソールからカスタムセキュリティポリシーを構成し、クライアントに適用します。

## 5. ネットワークのセキュリティ

### 1. ネットワークのアクセス管理

Larkはアマゾン ウェブ サービス（AWS）を使用して、サーバールーム、ネットワーク、サーバー、オペレーティングシステムなどを含むインフラストラクチャーや、インフラストラクチャーセキュリティに関するサービスを提供しています。AWSに基づいて、当社はサーバーアクセスにおけるセキュリティ制御を強化し、すべてのサービスは要塞マシンを介して操作および監査する必要があります。



社内のリソースにアクセスするには、従業員の認証が必要です。IDの認証後、従業員はデフォルトで最小限の権限を得ることができます。新しく許可を取得するには、関連責任者によって承認および記録される必要があります。許可には有効期限があり、システムは有効期限後に再度自動的に許可を得ることができます。従業員によるオンラインサービスの操作は要塞マシンを介して実行され、すべての操作ログは監査用に保持されます。

企業ネットワークの外にいる従業員は、VPN接続を介して企業の内部リソースにアクセスする必要があります。Larkの内部監査および管理部門は、アクセスログを監査し、プロトコル違反の記録を検索して、必要な処分を行います。

## 2. DDoS攻撃とサイバー攻撃からの防御

Larkサービスは、世界中のお客様にCDNやダイナミックな高速化によるネットワークへのアクセスと、AWSの負荷分散によるバックエンドサービスへのアクセスを提供します。DDoS攻撃が行われた場合、アカマイやAWSなどによるネットワーククリーニングサービスを通じて攻撃が防御されます。

## 3. ネットワーク通信の暗号化

Larkサービスは社内と外部のネットワークの両方で常にHTTPSとWSSを介して通信するので、通信プロセスのセキュリティが確保され、盗聴や改ざんが防止されます。

# 6. サーバーセキュリティ

Larkは、AWSのサーバーを使用してサービスを提供しています。

Amazonは、物理層から仮想化層までのクラウドサーバーセキュリティを提供します。AWSが提供するクラウドサーバーセキュリティの詳細については、Amazonクラウドセキュリティに関するホワイトペーパーをご参照ください。

[https://d1.awsstatic.com/whitepapers/Security/Security\\_Compute\\_Services\\_Whitepaper.pdf](https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf)

# 7. アプリケーションのセキュリティ

Larkは、開発のプロセスを保護するために適切な措置を講じます。

## 1. セキュリティ開発のプロセス

セキュリティに違反する原因からセキュリティリスクをコントロールするよう努めています。セキュリティの学習コースを作成し、オンサイトおよびオンラインでのトレーニングを実施しています。すべての開発者と製品マネージャーがセキュリティの脆弱性の原因を理解し、コーディングの知識を強化するためのセキュリティトレーニングを受けます。セキュリティチームは、プロジェクトの開始時にプロジェクトマネージャーと連絡を取り、セキュリティ要件とセキュリティテストがプロジェクト計画に反映されていることを確認します。それと同時に、セキュリティチームはサプライチェーンによって脆弱性が発生しないように製品に使用されるサードパーティのライブラリとツールを評価します。セキュリティチームは製品チームと協力し、設計とコーディングのセキュリティレビューを実施します。製品がオンラインで使用される前にサービスのセキュリティを確保するために、導入のペネトレーションテストとセキュリティ評価を行います。

## 2. ユーザーアカウントのセキュリティ

Larkシステムへのユーザーのアクセスは、パスワードと動的な認証コードを使用して認証されます。これにより、パスワードの紛失によるアカウントの漏えいを効果的に回避できます。認識されないデバイスでログインした場合、リスク管理戦略により、ユーザーのログイン認証の難易度を上げます。同時に、アカウントシステムには、異常で脅威の可能性があるログイン試行に対する防御機能を備えています。リスク管理システムには、悪意のある登録や認証情報リスト型攻撃の防止などの保護機能があります。

## 3. 脆弱性と緊急対応

セキュリティチームは外部から報告された脆弱性をレビューしそれらを修正するため、その脆弱性がもたらす被害と緊急性を評価します。

Larkはサービスとオペレーティングシステムを定期的にスキャンし、脆弱性が検出した場合はサービスを修復します。

当社のセキュリティチームは、サードパーティの評価企業やホワイトハットコミュニティと緊密に連携し、定期的にコミュニケーションをとっています。また、外部の企業やホワイトハットに、セキュリティの脆弱性を発見することに対する報酬付きで、侵入テストを実施するよう招待することがあります。

当社のセキュリティチームは、24時間365日の緊急対応戦略を実施しています。セキュリティインシデントが発生すると、セキュリティチームは緊急時対応計画に従ってインシデントの種類をすばやく分類し、被害の拡大を防ぐために緊急対応プロセスを開始します。

# 8. データセキュリティ

Larkには、データライフサイクルの各段階（作成、保存、利用、通信、共有、長期保管、破棄など）の技術的保証を備えた完全なデータライフサイクル管理プロセスがあります。

## 1. データ通信

当社は、ユーザーに安全な暗号化プロトコルをサポートするデータ伝送チャネルを提供します。メッセージプル、識別認証、操作指示などのデータ送信は、HTTPSおよび2048ビットのRSA暗号化キーを使用して暗号化されます。メッセージプッシュはWSSプロトコルを使用し、送信データを暗号化により保護します。クラウドドキュメントサービスは共通鍵暗号アルゴリズムAES256を使用して暗号化し、送信されます。

## 2. データストレージ

Larkは、キーメカニズムを使用して暗号化されたデータストレージのサポートをしています。

Larkは包括的なデータ分類と管理方法を開発し、Larkスイートによって収集されたユーザー情報を厳密に分類しました。Larkはシステムに保存されている機密データを暗号化しているため、



ユーザー情報を効果的に保護できます。

KMSサービスは、キーのライフサイクル管理と、作成、保存、利用、更新、共有、破棄などの重要な設定情報の管理をします。Larkユーザーのデータ暗号化およびLarkサービスの他のさまざまな機密情報（データベースアカウント、パスワードなど）に使用されるマスターキーは、KMSシステムに保存され、Larkにより管理され、KMSインターフェイスを介してアクセスが実行されます。キーが初期化されると、KMSシステムはシャミアの秘密分散プロトコルを使用して5つの重要なコンポーネントを生成し、それらは管理を行うさまざまな機能に分配されます。KMSシステムのマスターキーは、3つ以上のキーコンポーネントを提供する場合にのみ復元することができます。KMSマスターキーは、KMSのセキュリティを向上させるために定期的に更新されます。

### 3. データアクセス

ユーザーデータへのアクセスは、アクセス許可によって厳密に分離されます。ユーザーは、許可なしに他のユーザーのアカウントにアクセスすることができません。共有などのデータへのアクセスは、データの所有者本人による明確な承認を通じて行われる必要があります。

当社の従業員によるユーザーデータへのアクセスは厳しく制限および監査されており、デフォルト設定により、従業員がユーザーデータにアクセスできないようになっています。特別なアクセス要件には、ユーザーによる明確な承認と、一時的にアクセスする権利を取得するための厳格な社内の承認プロセスが必要です。このプロセスでは、ユーザーは操作が完了するとアクセスの権限を失います。Larkのオンライン環境のすべてのサーバーのログインログ、操作ログ、サーバーセキュリティベースラインファイルの変更、およびアクセス許可の変更ログは記録されます。違法なアクセスおよびリスク操作のリアルタイム監査は自動検出によって実行され、アラームが生成されます。Larkはユーザーアクティビティのログを詳細に記録し、細かく役割を設けてそれぞれにオペレーターを用意し、それに応じてさまざまな権限を付与します。操作には承認と監査が必要です。

それぞれユーザーの同意を得ない限り、当社またはLarkはユーザーの情報を公開できません。ただし、法律、規制、強制的な行政執行または司法の要件に従ってユーザー情報が必要な場合は、当社またはLarkは、必要な個人データの種類、または開示の必要性に応じて、規制当局または法務当局にユーザーの個人情報を開示する場合があります。法令により承認された開示要求を受け取った場合、その条例に従った法的文書の発行が必要になります。当社は、法執行機関が特定の調査目的で取得するための法的な権利を有するデータのみを提供します。法律および規制に従い、開示する文書は暗号化によって保護されています。

### 4. データの削除

ユーザーへのサービスを終了する場合、Lark管理者はそのユーザーのアカウント情報を削除し、現地の法律および規制に従ってユーザーのデータを永久的に削除します。マウントされていないディスクは、ドライブ内に情報を残さないように消磁して破壊する必要があります。

辞任する従業員は、テナント管理者にアカウントの廃止申請を行います。テナント管理者は、退職した従業員のアカウント内のグループ所有者、

スケジュール、ドキュメント、およびその他のデータが転送されたことを確認した後、Larkカスタマーサービス機能を使用して当社に連絡します。当社は、テナント管理者の申請に基づいて、要求されたアカウントのデータとドキュメントの識別を解除します。

当社がユーザーとのサービス契約に署名することで、サービスの終了時にユーザーの要請に従い対応データが破棄されることに同意したとみなされます。

法人のテナントユーザーだけではなく、Larkスイートは個人ユーザーにもご利用いただけます。個々のユーザーが自分のアカウントを廃止する必要がある場合、ユーザーによる当社への申請が必要です。当社はLarkカスタマーサービス機能を使用して、アカウント廃止機能付きのLarkスイートインストールパッケージを提供します。インストール後、ユーザーはソフトウェアのアカウント廃止を申請することができ、それに応じてLarkスイートはバックエンドデータベース内のアカウントデータとドキュメントの識別を解除します。

## 8.5 データへの不正侵入検知

ログインの動作、オペレーションの操作、サーバーセキュリティベースラインファイルの変更、アクセス権の変更、およびオンライン上のすべてのサーバーのデータアクセスの動作は記録されます。セキュリティチームは、ユーザーの行動傾向と異常な行動モデルを定義することにより、異常な行動を監視および分析し、データへの不正アクセス、悪意のあるデータクロール、異常なログイン、権限の昇格など、異常なデータアクセス操作を自動的に検出します。セキュリティデバイスは、異常な動作を自動的に警告してブロックできます。

# 9. 物理インフラストラクチャーのセキュリティ

Larkは、アマゾン ウェブ サービスとアカマイを通じて、世界のさまざまな地域の顧客にサービスを提供しています。

## 1. アマゾン ウェブ サービス (AWS) インフラストラクチャーのセキュリティ

Larkのクラウドサービスプロバイダーの1つとして、AWSはクラウドサーバーなどのサービスを提供しています。AWSは、物理層から仮想化層までのすべてのハードウェアおよびソフトウェア機能を操作、管理、および制御します。Amazonは、世界をリードするクラウドサービスプロバイダーとして、ユーザーにインフラストラクチャーセキュリティを提供する業界トップのセキュリティ機能を備えています。AWSが提供するクラウドサービスインフラストラクチャーの保護に関する詳細については、AWSセキュリティホワイトペーパーをご参照ください：

[https://d0.awsstatic.com/whitepapers/Security/AWS\\_Security\\_Whitepaper.pdf](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf)

## 2. アカマイ インフラストラクチャーのセキュリティ

アカマイは、世界最大のCDNサービスプロバイダーであり、世界中で長期的な信頼性と安定したアクセラレーションサービスを提供しています。Larkはアカマイを通じて、海外の顧客に高速なアクセスを提供しています。アカマイのセキュリティに関する詳細については、アカマイセキュリティホワイトペーパーをご参照ください：

<https://www.akamai.com/cn/zh/about/ourthinking/white-papers.jsp>

## 10. 障害回復とサービス継続性

### 1. バックアップと障害回復

当社は、Larkスイートのバックアップ戦略、バックアップデータの保持、およびリカバリテストの方法などを標準化するために、データバックアップやリカバリ管理に関する方針を確立しています。ビジネスデータベースには定期的なスナップショットとバックアップがあり、データは2つの場所に保存され、3つの予備があります。さらに、データバックアップの整合性確保のために、バックアップパフォーマンスを監視するメカニズムを展開しています。Larkチームは定期的にバックアップデータのリカバリーテストを実施しています。

### 2. サービス継続性の保証

サービスシステムのアクセス層には、Larkが提供するパブリックゲートウェイサービスを介して高可用性モードでアクセスします。バックエンドはマルチインスタンスアクセスを使用し、サービスの信頼性を確保します。詳細な監視を通して、トラフィックのバーストまたは障害が発生した場合は、品質を落とした動作モードを使用することでサービスの可用性を確保します。

Larkは、ビジネスの損害につながる可能性のあるシナリオへの緊急時の対応と復旧対策のガイドラインを定めています。Larkは年に1度、ビジネス影響分析とリスク評価を実施し、当社のビジネスとリソースの損害を引き起こす可能性のある重要なプロセスと脅威を特定しています。また、最大許容停止時間、目標復旧時間、最小サービスレベルなどの指標を定義し、さまざまなビジネスラインの中断シナリオに対するそれぞれの対応戦略を開発しています。

### 3. 緊急訓練

当社には完全な緊急訓練メカニズムがあり、開発チーム、セキュリティチーム、運用、保守チームなどの参加者と定期的に障害訓練を実施しています。

## 11. 変更管理

### 1. プログラムの変更

当社は、変更計画の確立、変更の承認、変更の実施など、変更管理の要件と手順を定義する変更管理規則を制定しています。変更には、オンラインサービスの安定性、可用性、セキュリティに潜在的なリスクがあります。開発によるサービスへの影響を防ぐため、Larkは変更を厳格に制御しています。オンライン操作には、操作の適用を必要とし、承認を得た場合のみ操作できます。リリースは、サービスの安定性とセキュリティを確保するために、少量のトラフィックでテストする必要があります。

## 2. ソースコードの管理

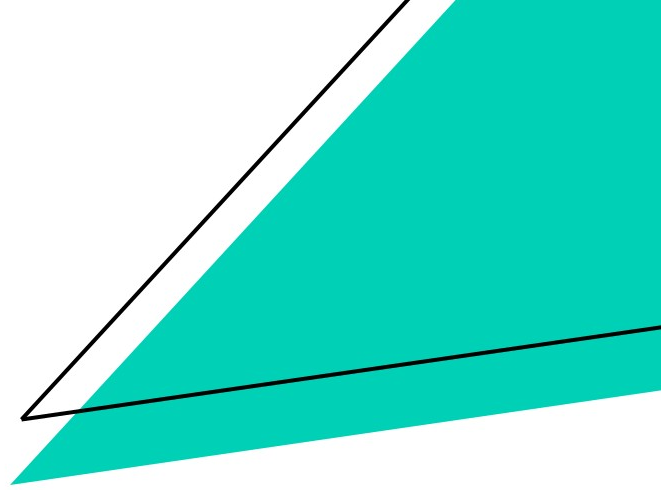
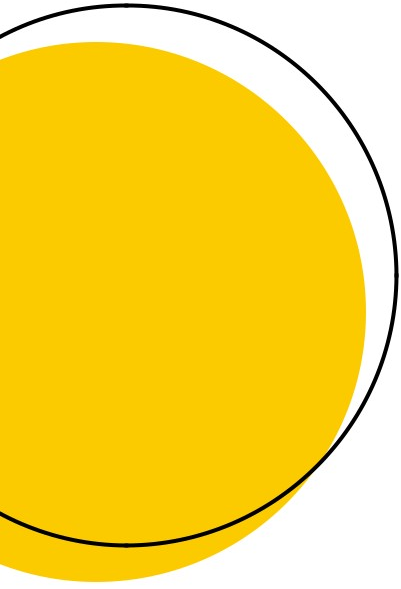
Larkは、厳密なソースコード管理プロセスを開発しており、開発者はチームに対応するコードウェアハウスにのみアクセスして管理できます。R&D担当者は、自分のグループのみに属するコードウェアハウスにアクセスできます。特定のコードウェアハウスの所有者は、プロジェクトごとの設定が必要です。R&D担当者が別のチームに属するコードウェアハウスへのアクセスを申請する場合、その申請はコードウェアハウス内で行われる必要があります。コードウェアハウスは、申請者のチームリーダーと適用されたコードウェアハウスの所有者から承認を受け取ると、申請者へのアクセスを自動的に許可します。

## 3. ITインフラストラクチャーの変更

Larkは、パブリックネットワーク境界にアクセス制御リスト（ACL）を展開することにより、ネットワークアクセスを管理します。ACL構成ベースラインとネットワークアクセス制御ポリシーを変更する必要がある場合、運用担当者はシステムワークフロープラットフォームに申請を上げます。システム部門のエンジニアは、変更実施の前に変更要求の合理性を評価します。システム部門の認定エンジニアのみが、ネットワークアクセス構成を変更するためのアクセス権を付与されています。

## 4. モニタリングの変更

内部監査は、変更管理に関連する統制を含む当社の内部統制システムの運用上の有効性を評価するために、毎年Larkによって実施されます。監査結果は、内部監査レポートに要約されます。監査によって例外が特定された場合、内部監査および内部統制部門は担当チームに修復措置を講じるよう通知し、修復ステータスを追跡します。変更の開発、テスト、承認、移行、および監視を含む変更管理のプロセスには、互換性のない責任の分離が存在します。



[www.larksuite.com](http://www.larksuite.com)

